CLAIMS

What is claimed is:

1 A method for evidencing payment of indicia using secret key cryptography in a system including a plurality of indicia generating devices that are divided into groups, each of the indicia generating devices for generating and printing indicia on a media that is to be received at a plurality of establishments, wherein the establishments are associated with different geographic designations, the method comprising the steps of:

(a) assigning a plurality of verification keys to each indicia generating device in each of the groups, wherein each of the verification keys assigned to each of the groups is encrypted as a function of a respective geographic designation;

(b) associating a key ID with each of the verification keys and encrypting each key ID as a function of the same geographic designation used to encrypt the corresponding verification key;

(c) distributing to each one of the establishments, the verification keys and the key ID's that were encrypted as a function of the geographic designation associated with the establishment;

(d) using one of the indicia generating devices to generate indicia for media destined for a particular one of the establishments, and evidencing the indicia by

(i) generating one of the verification keys and the corresponding key ID

assigned to indicia generating device's group based on the geographic designation associated with the particular establishment, and

(ii) using the generated verification key to create a digital signature, and digitally signing the indicia by including the digital signature and the generated key ID in the indicia; and

(e) upon receiving the media at the particular establishment, verifying the indicia on the media using the key ID on the indicia and the distributed verifications keys to compute a digital signature, and comparing the computed digital signature with the digital signature on the indicia.

2 The method of claim 1 further including the steps of:

assigning a secret key to each of the groups, and

encrypting the verification keys assigned to each group as a function of the secret key and the different geographic designations.

3 The method of claim 2 further including the steps of:

generating a master key; and

encrypting the key ID as a function of the master key, the geographic designation, and a designation of the group.

4 The method of claim 3 further including the step of generating and printing indicia for postage on a mail piece that is to be received at a plurality of distribution centers.

5 The method of claim 4 further including the step of verifying the indicia at a destination distribution center.

6 The method of claim 4 further including the step of verifying the indicia at an originating distribution center.

7 The method of claim 3 further including the step of using zip codes to represent the geographic designations.

8 The method of claim 1 further including the step of generating and printing indicia for tickets.

9 A method for evidencing payment of postage using secret key cryptography in a system including a plurality of postage generating devices that are divided into groups, each of the postage generating devices for generating postage indicia for mail destined for predetermined postal destinations, the method comprising the steps of:

(a) assigning a plurality of verification keys to each indicia generating device in each of the groups, wherein each of the verification keys assigned to each of the groups is encrypted as a function of a respective ;

(b) associating a key ID with each of the verification keys and encrypting each key ID as a function of the same destination used to encrypt the

corresponding verification key;

(c) requiring that verifiers of the postage indicia perform postal verification at the plurality of destinations, where each verifier services a respective destination;

(d) distributing to each respective destination verifier, the verification keys and the key ID's that were encrypted as a function of the corresponding destination; and

(e) requiring each of the postage generating devices to evidence the postage indicia for a mail piece destined for a particular destination by

(i) generating one of the verification keys and the corresponding key ID assigned to its group based on that particular destination, and

(ii) using the generated verification key to create a digital signature, and digitally signing the indicia by including the digital signature and the generated key ID on the indicia, such that when the mail is received at the predetermined destination, the verifier uses the key ID on the indicia and the distributed verifications keys to compute a digital signature, and compares the computed digital signature with the digital signature on the postage indicia to verify the postage indicia.

10 The method of claim 9 further including the steps of:

assigning a secret key to each of the groups, and

encrypting the verification keys assigned to each group as a function of the secret key and the plurality of destinations.

11 The method of claim 10 further including the steps of:

generating a master key; and

encrypting the key ID as a function of the master key, the destination, and a designation of the group.

12 The method of claim 11 further including the step of performing postage verification onsite at a destination distribution center.

13 The method of claim 12 further including the step of performing postage verification by a third party that is in remote communication with the destination distribution center.

14 The method as in claim 13 wherein the verifier further performs the steps of using the key ID to retrieve the corresponding verification key used to originally create the digital signature.

15 A system for evidencing payment of postage using secret key cryptography, comprising:

a plurality of postage generating devices that are divided into groups, each of the postage generating devices for generating postage indicia for mail destined for predetermined postal destinations;

a plurality of distribution centers for verifying the postage indicia, where each distribution center services at least one of the postage destinations; and

a key distribution center in communication with the plurality of postage generating

devices and with the plurality of distribution centers, the key distribution center for performing the functions of:

assigning a plurality of verification keys to each indicia generating device in each of the groups, wherein each of the verification keys assigned to each of the groups is encrypted as a function of a respective destination, and for associating a key ID with each of the verification keys and encrypting each key ID as a function of the same destination used to encrypt the corresponding verification key, and

distributing to each of the plurality of distribution centers, the verification keys and the key ID's encrypted as a function of the destination the distribution center services,

wherein in response to a request to generate indicia for a mail piece destined for a particular destination, each of the postage generating devices generates one of the verification keys and the corresponding key ID assigned to its group based on that particular destination, and uses the generated verification key to create a digital signature for the indicia, such that when the mail is received at the distribution center servicing the predetermined destination, the key ID from the indicia and the verification keys distributed to the distribution center are used to verify the digital signature on the postage indicia.

16 The system of claim 15 wherein the key distribution center further generates a master key, and a secret key for each of the postage generating devices groups, and distributes the

master key and the secret key to the respective postage generating devices within each of the groups.

17 The system of claim 16 wherein the verification keys assigned to each group are encrypted as a function of the secret key and the plurality of destinations.

18 The system of claim 17 further wherein the key ID is encrypted as a function of the master key, the destination, and a designation of the group.

19 The system of claim 18 wherein verification of the postage is performed onsite at the destination distribution centers.

20 The system of claim 19 wherein verification of the postage is performed by a third party that is in remote communication with the destination distribution centers.

21 The system as in claim 20 wherein the indicia is verified by using the key ID from the indicia to retrieve the corresponding verification key used to originally create the digital signature, wherein the retrieved verification key is used to compute the digital signature for the indicia and the computed digital signature is compared with the digital signature from the indicia.

22 A computer-readable media containing program instructions for evidencing payment of postage using secret key cryptography in a system including a plurality of postage

generating devices that are divided into groups, each of the postage generating devices for generating postage indicia for mail destined for predetermined postal destinations from among a plurality of destinations, the program instructions for:

(a) assigning a plurality of verification keys to each indicia generating device in each of the groups, wherein each of the verification keys assigned to each of the groups is encrypted as a function of a respective destination;

(b) associating a key ID with each of the verification keys and encrypting each key ID as a function of the same destination used to encrypt the corresponding verification key;

(c) requiring that verifiers of the postage indicia perform postal verification at the plurality of destinations, where each verifier services a respective destination;

(d) distributing to each respective destination verifier, the verification keys and the key ID's that were encrypted as a function of the corresponding destination; and

(e) requiring each of the postage generating devices to evidence the postage indicia for a mail piece destined for a particular destination by

(i) generating one of the verification keys and the corresponding key ID assigned to its group based on that particular destination, and

(ii) using the generated verification key to create a digital signature, and digitally signing the indicia by including the digital signature and the generated key ID on the indicia, such that when the mail is received at the predetermined destination, the verifier uses the key ID on the indicia and the distributed verifications keys to compute a digital

signature, and compares the computed digital signature with the digital signature on the postage indicia to verify the postage indicia.

23 The computer-readable media of claim 22 further including the instructions of:

assigning a secret key to each of the groups, and

encrypting the verification keys assigned to each group as a function of the secret key and the plurality of destinations.

24 The computer-readable media of claim 23 further including the instructions of:

generating a master key; and

encrypting the key ID as a function of the master key, the destination, and a designation of the group.

25 The computer-readable media of claim 24 further including the instruction of performing postage verification onsite at a destination distribution center.

26 The computer-readable media of claim 25 further including the instruction of performing postage verification by a third party that is in remote communication with the destination distribution center.

27 The computer-readable media as in claim 26 further including the instructions of using the key ID to retrieve the corresponding verification key used to originally create the digital signature.

28 A method for generating and distributing cryptographic keys for postage evidencing and verification in a system where mail is destined for predetermined postal destinations , wherein each of the postal destinations is serviced by a postal distribution center, the method comprising the steps of:

(a) creating a master secret key K;

(b) dividing a plurality of postage generating devices (PGDs) that generate postage indicia for mail into n groups G_i, $i = 1,...n$;

(c) assigning each PDG group, G_i, a secret key K_i;

(d) generating a set of n verification keys, $V_i^{Dest}, i = 1,...,n$, for each PGD group G_i, where each of the verification keys is calculated as a function of a respective postal destination (Dest);

(e) generating a set of key ID's, $I_i^{Dest}, i = 1,...,n$, where each key ID corresponds to one of the verification keys and is also generated as a function the same postal destination used to calculate the corresponding verification key;

(f) transferring to each distribution center, the verification keys V_i^{Dest} and key ID's I_i^{Dest} that were calculated as a function of the destination serviced by the distribution center; and

(g) transferring the master secret key K and the secret key K_i to all PGD's in group G_i, such that each PGD, when evidencing indicia for the mail destined for one of the predetermined postal destination, generates one of the verification keys based on the predetermined postal destination to create a

digital signature for the indicia.

29 The method of claim 28 further including the step of computing each verification key V_i^{Dest} as a one-way function H of the PGD group key K_i and a designation of the postal destination:

$$V_i^{Dest} = H(K_i, Dest).$$

30 The method of claim 29 further including the step of using ZIP codes to designate the plurality of postal destinations.

31 The method of claim 30 further including the step of computing each of the key ID's as a one-way function H of the PGD group, G_i, the master secret key, K, and a designation of the postal destination, *Dest*:

$$I_i^{Dest} = H(K, Dest, G_i).$$

32 A method for verifying postage indicia a mail piece received at a postal distribution center that services a particular postal region, comprising the steps of:

(a) receiving and storing a set of verification keys V_i^{Dest} and a set of key ID's I_i^{Dest} identifying the verification keys, wherein the verification keys and the key ID's were generated as a function of the postal region;

(b) in response to receiving the mail piece, determining the mail piece's postal region;

(c) if the distribution center is not within the mail piece's destination region, transferring the mail piece to the distribution center within the mail piece's postal region; and

(d) if the distribution center is within the mail piece's postal region, verifying the postage indicia by

(i) reading a digital signature and a key ID from the indicia,

(ii) using the key ID read from the indicia to retrieve the corresponding verification key from the stored set of verification keys,

(iii) using the retrieved verification key to compute a digital signature for the indicia, and

(iv) comparing the computed digital signature with the digital signature read from the postage indicia to verify the indicia.

33 The method of claim 32 further including the step of determining the mail piece's postal region based on a zip code.

34 The method of claim 33 further including the step of determining the mail piece's postal region based on a destination zip code.

35 The method of claim 33 further including the step of determining the mail piece's postal region based on a return address zip code.